MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2018/2019

TSN3251 – COMPUTER SECURITY

(All sections / Groups)

04 MARCH 2019
9.00 a.m - 11.00 a.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of **EIGHT pages (excluding this page)** with **FIVE questions.**

2. Answer all **FIVE** questions. Each question carries **20 marks** and the distribution of the marks for each subdivision is given. Maximum allotted are **100 marks.**

3. Please write all your answers in the Answer Booklet provided.

*Answer all **FIVE** questions. Each question carries 20 marks and the distribution of the marks for each subdivision is given.* ***(5 × 20=100 marks)***

QUESTION 1:

a. Explain briefly the following **principles of computer security**.

(i) Integrity (ii) Authentication (iii) Access Control

(6 marks)

b. State any TWO methods that can be used by the attacker in **Ciphertext-only cryptanalytic attacks** and specify how the attack can be prevented on each such method. **(4 marks)**

c. Specify the TWO conditions on which a cipher can be called as a **'computationally secure'** cipher. **(2 marks)**

d. Draw the basic model for **'Symmetric Cryptosystem'** to provide confidentiality. **(4 marks)**

e. Answer the following with respect to a class consisting of 60 students and a lecturer. Assume the **usage of asymmetric cryptosystem**.

(i) Identify the number of public and private keys needed if all the students in the group wish to send secret messages to each other without involving the lecturer. **(2 marks)**

(ii) Identify the number of public and private keys needed in a scheme, where messages cannot be sent between the two students directly and they can be routed only through the lecturer. **(2 marks)**

Continued...

QUESTION 2:

a. Assume that plaintext and ciphertext characters are represented as numerical values in Z_{26} as follows:

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Answer the following questions:

(i) Use **Hill Cipher** to encrypt the following plaintext.

secure

Use the following key for encryption.

$$K = \begin{bmatrix} 5 & 3 & 1 \\ 3 & 9 & 5 \\ 4 & 6 & 12 \end{bmatrix}$$

(6 marks)

(ii) Use **Affine Cipher** to decrypt the following ciphertext with $\mathbf{k_1=7}$ and $\mathbf{k_2=10}$ in **modulus 26,** where the key k_1 is used with multiplicative cipher and the key k_2 is used with additive cipher.

KOQ **(3 marks)**

(iii) Use **Vigenère Cipher to** decrypt the ciphertext "**SBHFWM**" using the 4-character keyword "LIVE". **(3 marks)**

b. (i) Construct a **Playfair matrix** with the key *gentle.* **(2.5 marks)**

(ii) Using the constructed Playfair matrix, encrypt the following message. Use 'z' as the filler character, if needed.

behaviour **(2.5 marks)**

c. Receiver gets the ciphertext message "**VBLEIEUENOYIXREFLS**". Assume the sender and receiver have agreed on the following:

Division of the text into blocks of characters and permute the characters in each group based on keyed transposition cipher.
Usage of Encryption Key: **2 6 3 5 4 1**
Usage of filler character as '**x**' if needed.

(i) Identify the **decryption key.** **(1 mark)**
(ii) Identify the **plaintext** at the receiving end. **(2 marks)**

Continued...

QUESTION 3:

a. For **Data Encryption Standard (DES)**, answer the following questions with respect to the first round of the encryption process.

Assume that the **32-bit Right Half (R_0)** obtained after passing the plaintext through the Initial Permutation Table is given as

$$R_0 = (1010\ \ 1011\ \ 1100\ \ 1101\ \ 0111\ \ 0110\ \ 0101\ \ 0100)_2$$

Assume also that the **48-bit first round sub-key (K_1)**, produced after passing the 64-bit key through Permuted Choice One (PC-1), left circular shift and Permuted Choice Two (PC-2), is given as

$$K_1 = (110000\ \ 110001\ \ 110010\ \ 110011\ \ 110100\ \ 110101\ \ 110110\ \ 110111)_2$$

(i) Expand R_0 using the following Expansion Permutation (E) Table to get **48-bit E [R_0]**. **(4 marks)**

Expansion Permutation (E) Table

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(ii) Calculate **A = E[R_0] XOR K_1** using the 48-bit result obtained in (i) and the given 48-bit first round sub-key. **(2 marks)**

b. One of the criteria for S-box design for **Data Encryption Standard (DES)** is given below:

> **"If two inputs to an S-box differ in the first two bits (bits 1 and 2) and same in the last two bits (5 and 6), the two outputs must be different. The middle bits can be arbitrary bits"**

Test the above criteria by applying the pair of inputs, **101110** and **010110**, separately to S-box 1.

(4 marks)

Continued...

Definition of S-box 1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

c. With reference to **Advanced Encryption Standard (AES)**, answer the following:

If ***a*** and ***b*** are two bytes, prove the nonlinearity of the **SubBytes transformation** by performing the following operation.

SubBytes $(a \oplus b) \neq$ **SubBytes** $(a) \oplus$ **SubBytes** (b)

Use SubBytes Transformation table given below and the values.

$a = (1001\ 0011)_2$ *and* $b = (0110\ 1101)_2$

(4 marks)

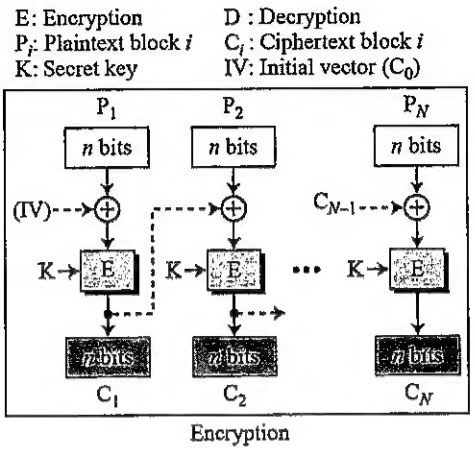
Note:

Substitute Bytes Transformation Table (AES S-Boxes)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	CB	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Continued...

d. With reference to the following diagram that shows the encryption process for **Cipher Block Chaining (CBC) mode** to be used with modern block ciphers for enciphering text of any size, answer the following:



Encryption

(i) Modify the above diagram to show the **decryption process.** **(2 marks)**

(ii) State the relation between plaintext and ciphertext blocks using **encryption** and **decryption** equations. **(2 marks)**

(iii) Assume that there are a total of 20 blocks and bit 32 in ciphertext block 12 is corrupted during transmission. Identify the **plaintext blocks along with the number of bits in each block** likely to be affected by this. Assume the underlying block cipher used is AES-128. **(2 marks)**

Continued...

QUESTION 4:

a. With reference to **Rivest-Shamir-Adleman (RSA)** cryptosystem, answer the following:

(i) Identify the **public key {e,n} and private key {d,n}** for the following data using RSA_Key_Generation algorithm given below. **(6 marks)**

p=31; q=61; e=23

where
p and q are two prime numbers
e is an integer with gcd (φ (n) , e) =1; 1 < e < φ (n);

```
RSA_Key_Generation
{
   Select two large primes p and q such that p ≠ q.
   n ← p × q
   ϕ(n) ← (p − 1) × (q − 1)
   Select e such that 1 < e < ϕ(n) and e is coprime to ϕ(n)
   d ← e^−1 mod ϕ(n)                    // d is inverse of e modulo ϕ(n)
   Public_key ← (e, n)                  // To be announced publicly
   Private_key ← d                      // To be kept secret
   return Public_key and Private_key
}
```

(ii) With the help of the following algorithms, perform **encryption** using the keys derived in (i) and using the plaintext message **P=3.** **(4 marks)**

```
RSA_Encryption (P, e, n)                // P is the plaintext in Z_n and P < n
{
   C ← Fast_Exponentiation (P, e, n)    // Calculation of (P^e mod n)
   return C
}
```

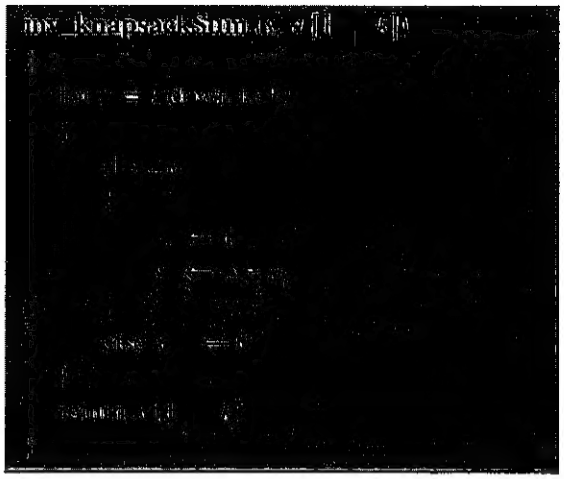
```
Square_and_Multiply (a, x, n)
{
   y ← 1
   for (i ← 0 to n_b − 1)               // n_b is the number of bits in x
   {
      if (x_i = 1)   y ← a × y mod n    // multiply only if the bit is 1
      a ← a^2 mod n                     // squaring is not needed in the last iteration
   }
   return y
}
```

Continued...

b. With reference to **inv-knapsackSum** algorithm given below, find the elements of a, which are to be dropped in the knapsack for the following data:

Predefined tuple: a = [3 4 7 15 30 60 120 240];
Sum of elements in the knapsack, s=101.

(2 marks)



c. State the difference between polymorphic and metamorphic viruses.

(2 marks)

d. Identify the **type of malware** for the following situation. Briefly explain your answer.

An employee plays a computer game during working hours. Assume that the game has a secret feature so that it pops an image of a word document on the screen, whenever he/she hits Shift-Ctrl on the keyboard. This employee uses this feature whenever the superior walks by while he/she is playing.

(2 marks)

e. State and briefly explain the FOUR basic steps that should be used to **secure an operating system.** **(4 marks)**

Continued...

QUESTION 5:

a. Briefly explain the concept of **cascading authorizations** with an example, in reference to database access control. **(2+2=4 marks)**

b. Briefly explain the **two-phase commit protocol** employed by most databases that can be used to achieve database integrity and availability. **(4 marks)**

c. Consider the following table related to **statistical database.**

Name	Sex	Department	Position	Salary (K) RM
A	Male	IT	Prof	14
B	Male	Electronics	Prof	12
C	Female	Electronics	Prof	13
D	Female	IT	Prof	10
E	Male	Mechanical	Prof	11
F	Female	Mechanical	Prof	10
G	Male	IT	Admin	4
H	Male	Electronics	Prof	12
I	Female	IT	RA	3
J	Male	Mechanical	Admin	5
K	Female	Electronics	Prof	15
L	Male	IT	RA	2

Answer the following.

(i) Assume that there is **no 'query size' restriction** and that a questioner knows that D is a female IT professor. Show a sequence of two queries that the questioner could use to determine D's salary.

(ii) Suppose that there is a **lower query size limit of 2, but there is no upper limit.** Show a sequence of queries that could be used to determine D's salary. Note: 'NOT' Operation can be used to overcome the lower query size limit.

(2+2=4 marks)

d. Briefly explain the following types of security threats.
(i) Port scanning
(ii) IP Address spoofing
(iii) SYN flooding

(2+2+2=6 marks)

e. State any FOUR basic steps involved in security risk analysis. **(2 marks)**

END OF EXAM